Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 14/11/2024 - 18/11/2024

Contents

1 Common Vulnerabilities and Exposures (CVE)

CVEs

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	Συσκευές/Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-48967	10	Baxter Life 2000 Ventilator (Homecare)	Insufficient Logging	N/A	N/A	https://www.baxter.com/healthcare-professionals/respiratory-care/life-2000-ventilator-homecare https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-319-01
https://nvd.nist.gov/vuln/detail/CVE-2024-52408	9.9	Team PushAssist Push Notifications for WordPress	Unrestricted Upload of File with Dangerous Type	from n/a through 3.0.8	N/A	https://pushassist.com/push-notifications-for-wordpress/ https://patchstack.com/database/vulnerability/push-notification-for-wp-by-pushassist/wordpress-push-notifications-for-wordpress-by-pushassist-plugin-3-0-8-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-52403	9.9	WPExperts User Management (Wordpress)	Unrestricted Upload of File with Dangerous Type	from n/a through 1.1	N/A	https://wordpress.org/plugins/user-management/ https://patchstack.com/database/vulnerability/user-management/wordpress-user-management-plugin-1-1-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-20036	9.9	Cisco IND	OS Command Injection	N/A	N/A	https://www.cisco.com/c/en/us/products/cloud-systems-management/industrial-network-director/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-CAeLFk6V
https://nvd.nist.gov/vuln/detail/CVE-2024-52369	9.9	Optimal Access Inc. Kbucket	Unrestricted Upload of File with Dangerous Type	from n/a through 4.1.6	N/A	https://optimalaccess.com/ https://patchstack.com/database/vulnerability/kbucket/wordpress-kbucket-plugin-4-1-6-arbitrary-file-upload-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2023-43091	9.8	GNOME Maps	Cross-site Scripting	N/A	N/A	https://apps.gnome.org/en/Maps/ https://gitlab.gnome.org/GNOME/gnome-maps/-/issues/588
https://nvd.nist.gov/vuln/detail/CVE-2024-8856	9.8	WP Time Capsule plugin for WordPress	Unrestricted Upload of File with Dangerous Type	all versions up to, and including, 1.22.21	N/A	https://wordpress.org/plugins/wp-time-capsule/ https://www.wordfence.com/threat-intel/vulnerabilities/id/fdc2de78-5601-461f-b2f0-c80b592ccb1b?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10934	9.8	OpenBSD	Double Free	7.5 before errata 008 7.4 before errata 021	N/A	https://www.openbsd.org/ https://ftp.openbsd.org/pub/OpenBSD/patches/7.4/common/021_nfs.patch.sig https://ftp.openbsd.org/pub/OpenBSD/patches/7.5/common/008_nfs.patch.sig

https://nvd.nist.gov/vuln/detail/CVE-2024-45971	9.8	MZ Automation Lib IEC61850	Classic Buffer Overflow	before commit 1f52be9ddeae00e69cd43e4cac3cb4f0c880c4f0	N/A	https://libiec61850.com/documentation/iec-61850-client-tutorial/ https://encs.eu/news/critical-security-vulnerabilities-discovered-in-mz-automations-mms-client/ https://github.com/mz-automation/libiec61850/commit/1f52be9ddeae00e69cd43e4cac3cb4f0c880c4f0
https://nvd.nist.gov/vuln/detail/CVE-2024-10924	9.8	Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress	Authentication Bypass	9.0.0 to 9.1.1.1	N/A	https://el.wordpress.org/plugins/really-simple-ssl/ https://www.wordfence.com/threat-intel/vulnerabilities/id/7d5d05ad-1a7a-43d2-bbbf-597e975446be?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-11120	9.8	Certain EOL GeoVision devices	OS Command Injection	N/A	N/A	https://www.geovision.com.tw/products.php https://www.twcert.org.tw/en/cp-139-8237-26d7a-2.html
https://nvd.nist.gov/vuln/detail/CVE-2024-47533	9.8	Cobbler (Linux installation server)	Improper Authentication	3.0.0 and prior to versions 3.2.3 and 3.3.7	N/A	https://cobbler.github.io/ https://github.com/cobbler/cobbler/security/advisories/GHSA-m26c-fcgh-cp6h
https://nvd.nist.gov/vuln/detail/CVE-2024-52316	9.8	Apache Tomcat	Unchecked Error Condition	from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9.0.95	11.0.0, 10.1.31 or 9.0.96	https://tomcat.apache.org/ https://lists.apache.org/thread/lopzlqh91jj9n334g02om08sbysdb928
https://nvd.nist.gov/vuln/detail/CVE-2024-11315	9.8	DVC from TRCore	Relative Path Traversal	N/A	N/A	https://www.trcore.com.tw/en https://www.twcert.org.tw/en/cp-139-8255-0bb1a-2.html
https://nvd.nist.gov/vuln/detail/CVE-2024-11319	9.6	django CMS	Improper Neutralization of Input	3.11.7, 3.11.8, 4.1.2, 4.1.3	N/A	https://www.django-cms.org/en/ https://www.django-cms.org/en/blog/2024/11/13/django-cms-security-update/
https://nvd.nist.gov/vuln/detail/CVE-2024-11263	9.3	Global Pointer (GP) (Zephyr project)	Privilege Context Switching Error	N/A	N/A	https://github.com/zephyrproject-rtos/zephyr/ https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-jjf3-7x72-pqm9
https://nvd.nist.gov/vuln/detail/CVE-2023-20154	9.1	Cisco Modeling Labs	Authentication Bypass	N/A	N/A	https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-auth-bypass-4fUCCeG5
https://nvd.nist.gov/vuln/detail/CVE-2024-37285	9.1	Kibana	Deserialization of Untrusted Data	N/A	N/A	https://www.elastic.co/kibana https://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119
https://nvd.nist.gov/vuln/detail/CVE-2024-50306	9.1	Apache Traffic Server	Unchecked Return Value	from 9.2.0 through 9.2.5, from 10.0.0 through 10.0.1	9.2.6 or 10.0.2	https://trafficserver.apache.org/ https://lists.apache.org/thread/y15fh6c7kyqvzm0f9odw7c5jh4r4np0y

https://nvd.nist.gov/vuln/detail/CVE-2024-10728	8.8	Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress	Missing Authorization	all versions up to, and including, 4.1.16	N/A	https://wordpress.org/plugins/ultimate-post/ https://www.wordfence.com/threat-intel/vulnerabilities/id/076f36fb-c2fb-43e0-a027-1351d3995489?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-49060	8.8	Azure Stack HCI	Use of Hard-coded Credentials	N/A	N/A	https://azure.microsoft.com/en-us/products/azure-stack/hci https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49060
https://nvd.nist.gov/vuln/detail/CVE-2024-11248	8.8	Tenda AC10	Improper Restriction of Operations within the Bounds of a Memory Buffer	16.03.10.13	N/A	https://www.tendacn.com/gr/product/ac10v3.html https://tasty-foxtrot-3a8.notion.site/Tenda-AC10v4-formSetRebootTimer-stack-overflow-13d0448e619580bf8ab1df7cfb6c018b
https://nvd.nist.gov/vuln/detail/CVE-2024-10962	8.8	Migration, Backup, Staging – WPvivid plugin for WordPress	Deserialization of Untrusted Data	all versions up to, and including, 0.9.107	N/A	https://wordpress.org/plugins/wpvivid-backuprestore/ https://www.wordfence.com/threat-intel/vulnerabilities/id/9b4eba78-29f2-4357-ab3c-7bc3c20e0e75?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10979	8.8	PostgreSQL PL/Perl	External Control of System or Configuration Setting	before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21	N/A	https://www.postgresql.org/docs/current/plperl.html https://www.postgresql.org/support/security/CVE-2024-10979/
https://nvd.nist.gov/vuln/detail/CVE-2024-45505	8.8	Apache HertzBeat	Command Injection	before 1.6.1	1.6.1	https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2 https://lists.apache.org/thread/gvbc68krhqhht7mkkkx7k13k6k6fdhy0 https://lists.apache.org/thread/h8k14o1bfyod66p113pkgnt1s52p6p19
https://nvd.nist.gov/vuln/detail/CVE-2023-20125	8.6	Cisco BroadWorks Network Server	Uncontrolled Resource Consumption	N/A	N/A	https://www.cisco.com/c/en/us/support/unified-communications/broadworks-network-server/model.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-tcp-dos-KEdJCxLs
https://nvd.nist.gov/vuln/detail/CVE-2024-9186	8.6	Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit WordPress	SQL injection	before 3.3.0	N/A	https://wordpress.org/plugins/wp-marketing-automations/ https://wpscan.com/vulnerability/fab29b59-7e87-4289-88dd-ed5520260c26/
https://nvd.nist.gov/vuln/detail/CVE-2024-9693	8.5	GitLab CE/EE	Incorrect Authorization	from 16.0 prior to 17.3.7, starting from 17.4 prior to 17.4.4, and starting from 17.5 prior to 17.5.2	N/A	https://about.gitlab.com/install/ce-or-ee/ https://gitlab.com/gitlab-org/gitlab/-/issues/497449
https://nvd.nist.gov/vuln/detail/CVE-2024-49574	8.3	Zohocorp ManageEngine ADAudit Plus	SQL Injection	below 8123	N/A	https://www.manageengine.com/products/active-directory-audit/ https://www.manageengine.com/products/active-directory-audit/cve-2024-49574.html

https://nvd.nist.gov/vuln/detail/CVE-2024-52508	8.2	Nextcloud Mail	Exposure of Sensitive Information to an Unauthorized Actor	N/A	1.14.6, 1.15.4, 2.2.11, 3.6.3, 3.7.7 or 4.0.0	https://apps.nextcloud.com/apps/mail https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vmhx-hwph-q6mc
https://nvd.nist.gov/vuln/detail/CVE-2024-39726	8.2	IBM Engineering Lifecycle Optimization - Engineering Insights	Improper Restriction of XML External Entity Reference	7.0.2 and 7.0.3	10.0.18	https://www.ibm.com/docs/en/engineering-lifecycle-management-suite/lifecycle-optimization-insights/7.0.3?topic=overview https://www.ibm.com/support/pages/node/7176208
https://nvd.nist.gov/vuln/detail/CVE-2024-52867	8.1	GNU Guix	privilege escalation	before 5ab3c4c	N/A	https://guix.gnu.org/ https://guix.gnu.org/en/blog/2024/build-user-takeover-vulnerability/
https://nvd.nist.gov/vuln/detail/CVE-2024-40638	8.1	GLPI (IT management software package)	SQL Injection	N/A	10.0.17	https://glpi-project.org/ https://github.com/glpi-project/glpi/security/advisories/GHSA-8843-r3m7-gfqx
https://nvd.nist.gov/vuln/detail/CVE-2022-20649	8.1	Cisco RCM for Cisco StarOS Software	Active Debug Code	N/A	N/A	https://www.cisco.com/c/dam/en/us/td/docs/wireless/upc/21-28/rcm-config-admin/21-28-rcm-config-admin.pdf https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tetr-cmd-injc-skrwGO https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-FmbPu2pe
https://nvd.nist.gov/vuln/detail/CVE-2024-0875	8.1	openemr/openemr	Cross-site Scripting	7.0.1	N/A	https://www.open-emr.org/ https://github.com/openemr/openemr/commit/d141d2ca06fb2171a202c7302dd5d5af8539f255 https://huntr.com/bounties/16cba0fc-748d-4ea8-9573-1f6fbe9a27c9
https://nvd.nist.gov/vuln/detail/CVE-2024-45670	8.1	IBM Security SOAR	Weak Password Recovery Mechanism for Forgotten Password	51.0.1.0 and earlier	N/A	https://www.ibm.com/products/qradar-soar https://www.ibm.com/support/pages/node/7172206
https://nvd.nist.gov/vuln/detail/CVE-2024-8979	8	Essential Addons for Elementor – Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress	Exposure of Sensitive Information to an Unauthorized Actor	all versions up to, and including, 6.0.9	N/A	https://wordpress.org/plugins/essential-addons-for-elementor-lite/ https://www.wordfence.com/threat-intel/vulnerabilities/id/34d09086-be33-40cf-b5bf-d6c03cf0b68a?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-52308	8	GitHub CLI	Improper Neutralization of Special Elements	2.6.1 and earlier	N/A	https://cli.github.com/ https://github.com/cli/cli/security/advisories/GHSA-p2h2-3vg9-4p87

https://nvd.nist.gov/vuln/detail/CVE-2024-51141	7.8	TOTOLINK Bluetooth Wireless Adapter A600UB	Improper Validation of Integrity Check Value	A600UB	N/A	https://totolink.com.my/products/a600ub/ https://infosecwriteups.com/dll-hijacking-in-totolink-a600ub-driver-installer-13787c4d97b4
https://nvd.nist.gov/vuln/detail/CVE-2024-52945	7.8	Veritas NetBackup	execution of code	before 10.5	N/A	https://www.veritas.com/protection/netbackup https://www.veritas.com/content/support/en_US/security/VTS24-012
https://nvd.nist.gov/vuln/detail/CVE-2024-52436	7.6	Post SMTP Wordpress plugin	SQL Injection	from n/a through 2.9.9	N/A	https://wordpress.org/plugins/post-smtp/ https://patchstack.com/database/vulnerability/post-smtp/wordpress-post-smtp-plugin-2-9-9-sql-injection-vulnerability?_s_id=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-10645	7.5	Blogger 301 Redirect plugin for WordPress	SQL Injection	all versions up to, and including, 2.5.3	N/A	https://wordpress.org/plugins/blogger-to-wordpress-redirection/ https://www.wordfence.com/threat-intel/vulnerabilities/id/06359274-37ae-47f5-824c-25600c5b06eb?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-24452	7.5	Athonet vEPC MME (HP)	Out-of-bounds Read	v11.4.0	N/A	https://www.hpe.com/us/en/solutions/athonet.html https://cellularsecurity.org/ransacked http://athonet.com
https://nvd.nist.gov/vuln/detail/CVE-2024-49754	7.5	LibreNMS	Cross-Site Scripting	N/A	24.10.0	https://www.librenms.org/ https://github.com/librenms/librenms/security/advisories/GHSA-gfwr-xqmj-j27v
https://nvd.nist.gov/vuln/detail/CVE-2024-41784	7.5	IBM Sterling Secure Proxy	Path Traversal	6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, and 6.1.0.0	N/A	https://www.ibm.com/products/secure-proxy https://www.ibm.com/support/pages/node/7173631
https://nvd.nist.gov/vuln/detail/CVE-2022-20685	7.5	Snort	Integer Overflow or Wraparound	N/A	N/A	https://www.snort.org/ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-NXOxDhRQ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-9D3hJLuj
https://nvd.nist.gov/vuln/detail/CVE-2024-11237	7.5	TP-Link VN020	Improper Restriction of Operations within the Bounds of a Memory Buffer	F3v(T) TT_V6.2.1021	N/A	https://service-provider.tp-link.com/vdsl/vn020-f3/ https://github.com/Zephkek/TP-Thumper
https://nvd.nist.gov/vuln/detail/CVE-2024-45784	7.5	Apache Airflow	Debug Messages Revealing Unnecessary Information	before 2.10.3	N/A	https://airflow.apache.org/ https://github.com/apache/airflow/pull/43040
https://nvd.nist.gov/vuln/detail/CVE-2024-3760	7.5	lunary-ai/lunary	Allocation of Resources Without Limits or Throttling	1.2.7	N/A	https://lunary.ai/ https://huntr.com/bounties/c29e9f36-8261-463d-8862-7f4fdcc8eddc

https://nvd.nist.gov/vuln/detail/CVE-2024-8403	7.5	MELSEC iQ-F Series FX5-ENET	Improper Validation of Specified Type of Input	FX5-ENET versions 1.100 and later and FX5-ENET/IP versions 1.100 to 1.104	N/A	https://emea.mitsubishielectric.com/fa/products/cnt/plc/plcf/network-communication-module/fx5-enet.html# https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2024-009_en.pdf
https://nvd.nist.gov/vuln/detail/CVE-2024-21287	7.5	Oracle Agile PLM Framework	unauthorized access to critical data	9.3.6	N/A	https://www.oracle.com/scm/product-lifecycle-management/ https://www.oracle.com/security-alerts/alert-cve-2024-21287.html
https://nvd.nist.gov/vuln/detail/CVE-2024-52940	7.5	AnyDesk	Insertion of Sensitive Information into Log File	through 8.1.0	N/A	https://anydesk.com/en https://github.com/ebrasha/abdal-anydesk-remote-ip-detector
https://nvd.nist.gov/vuln/detail/CVE-2022-20853	7.4	Cisco Expressway Series and Cisco TelePresence VCS	Cross-Site Request Forgery	N/A	N/A	https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-thinrcpt-xss-gSj4CecU https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-SEjz69dv https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-sqpsSfY6 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-prv-esc-8PdRU8t8
https://nvd.nist.gov/vuln/detail/CVE-2024-7730	7.4	QEMU	Heap-based Buffer Overflow	N/A	N/A	https://www.qemu.org/ https://access.redhat.com/security/cve/CVE-2024-7730
https://nvd.nist.gov/vuln/detail/CVE-2024-52926	7.3	Delinea Privilege Manager	mishandles the security of the Windows agent	before 12.0.2	N/A	https://delinea.com/products/privilege-manager https://docs.delinea.com/online-help/privilege-manager/release-notes/12.0.2-combined.htm
https://nvd.nist.gov/vuln/detail/CVE-2024-10793	7.2	WP Activity Log plugin for WordPress	Cross-site Scripting	all versions up to, and including, 5.2.1	N/A	https://wordpress.org/plugins/wp-security-audit-log/ https://www.wordfence.com/threat-intel/vulnerabilities/id/44f3b2e4-c537-4369-b2d6-39fbc6cb8e08?source=cve

2 CISA/CERT-EU Alerts & Advisories

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες**	**URL**
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-9463 Palo Alto Networks Expedition OS Command Injection Vulnerability CVE-2024-9465 Palo Alto Networks Expedition SQL Injection Vulnerability CVE-2024-1212 Progress Kemp LoadMaster OS Command Injection Vulnerability CVE-2024-0012 Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability CVE-2024-9474 Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2024/11/14/cisa-adds-two-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/11/18/cisa-adds-three-known-exploited-vulnerabilities-catalog
CISA Releases Nineteen Industrial Control Systems Advisories	ICSA-24-319-01 Siemens RUGGEDCOM CROSSBOW ICSA-24-319-02 Siemens SIPORT ICSA-24-319-03 Siemens OZW672 and OZW772 Web Server ICSA-24-319-04 Siemens SINEC NMS ICSA-24-319-05 Siemens Solid Edge ICSA-24-319-06 Siemens SCALANCE M-800 Family ICSA-24-319-07 Siemens Engineering Platforms ICSA-24-319-08 Siemens SINEC INS ICSA-24-319-09 Siemens Spectrum Power 7 ICSA-24-319-10 Siemens TeleControl Server ICSA-24-319-11 Siemens SIMATIC CP ICSA-24-319-12 Siemens Mendix Runtime ICSA-24-319-13 Rockwell Automation Verve Asset Manager ICSA-24-319-14 Rockwell Automation FactoryTalk Updater ICSA-24-319-15 Rockwell Automation Arena Input Analyzer ICSA-24-319-16 Hitachi Energy MSM ICSA-24-319-17 2N Access Commander ICSA-24-291-01 Elvaco M-Bus Metering Gateway CMe3100 (Update A) ICSMA-24-319-01 Baxter Life2000 Ventilation System	https://www.cisa.gov/news-events/alerts/2024/11/14/cisa-releases-nineteen-industrial-control-systems-advisories

3 News

News	
Σύντομη περιγραφή / Τίτλος	**URL**
THN Recap: Top Cybersecurity Threats, Tools, and Practices (Nov 11 - Nov 17)	https://thehackernews.com/2024/11/thn-recap-top-cybersecurity-threats_18.html
NSO Group Exploited WhatsApp to Install Pegasus Spyware Even After Meta's Lawsuit	https://thehackernews.com/2024/11/nso-group-exploited-whatsapp-to-install.html
Microsoft 365 Admin portal abused to send sextortion emails	https://www.bleepingcomputer.com/news/security/microsoft-365-admin-portal-abused-to-send-sextortion-emails/
Major security audit of critical FreeBSD components now available	https://www.helpnetsecurity.com/2024/11/18/security-audit-freebsd-components/

3.1 Breaches

News - Breaches	
Σύντομη περιγραφή / Τίτλος	**URL**
AnnieMac Home Mortgage breach impacts 171K	https://www.scworld.com/brief/anniemac-home-mortgage-breach-impacts-171k
T-Mobile is one of the victims of the massive Chinese breach of telecom firms	https://securityaffairs.com/171127/apt/t-mobile-victim-chinese-breach-of-telco-firms.html

3.2 Vulnerabilities and flaws

News – Vulnerabilities and Flaws	
Σύντομη περιγραφή / Τίτλος	**URL**
Critical Really Simple Security plugin flaw impacts 4M+ WordPress sites	https://securityaffairs.com/171100/hacking/really-simple-security-plugin-flaw-affects-4m-sites.html
Palo Alto Networks confirmed active exploitation of recently disclosed zero-day	https://securityaffairs.com/171057/hacking/palo-alto-networks-zero-day-exploitation.html
Cybersecurity Flaws in US Drinking Water Systems Put 26 Million at Risk	https://hackread.com/cybersecurity-flaws-us-drinking-water-systems-risks/
Warning: DEEPDATA Malware Exploiting Unpatched Fortinet Flaw to Steal VPN Credentials	https://thehackernews.com/2024/11/warning-deepdata-malware-exploiting.html
8.8 Rated PostgreSQL Vulnerability Puts Databases at Risk	https://hackread.com/postgresql-vulnerability-puts-databases-at-risk/
Mirai Malware Spreads Via GeoVision Zero-Day Exploit	https://dailysecurityreview.com/security-spotlight/mirai-malware-spreads-via-geovision-zero-day-exploit/

VMware Discloses Exploitation of Hard-to-Fix vCenter Server Flaw	https://www.securityweek.com/vmware-discloses-exploitation-of-hard-to-fix-vcenter-server-flaw/

3.3 Potential threats / Threat intelligence

News – Potential Threats / Threat Intelligence	
Σύντομη περιγραφή / Τίτλος	**URL**
Iranian Hackers Deploy WezRat Malware in Attacks Targeting Israeli Organizations	https://thehackernews.com/2024/11/iranian-hackers-deploy-wezrat-malware.html
Surge in DocuSign Phishing Attacks Target US State Contractors	https://www.infosecurity-magazine.com/news/docusign-phishing-targets-us-state/
Fake Discount Sites Exploit Black Friday to Hijack Shopper Information	https://thehackernews.com/2024/11/fake-discount-sites-exploit-black.html
Vietnamese Hacker Group Deploys New PXA Stealer Targeting Europe and Asia	https://thehackernews.com/2024/11/vietnamese-hacker-group-deploys-new-pxa.html
Phishing emails increasingly use SVG attachments to evade detection	https://www.bleepingcomputer.com/news/security/phishing-emails-increasingly-use-svg-attachments-to-evade-detection/
Chinese hackers exploit Fortinet VPN zero-day to steal credentials	https://www.bleepingcomputer.com/news/security/chinese-hackers-exploit-fortinet-vpn-zero-day-to-steal-credentials/
New 'Helldown' Ransomware Variant Expands Attacks to VMware and Linux Systems	https://thehackernews.com/2024/11/new-helldown-ransomware-expands-attacks.html
APT41 expands cyberespionage to target Windows	https://www.scworld.com/brief/apt41-expands-cyberespionage-to-target-windows

3.4 Guides / Tools

News – Guides / Tools	
Σύντομη περιγραφή / Τίτλος	**URL**
ScubaGear: Open-source tool to assess Microsoft 365 configurations for security gaps	https://www.helpnetsecurity.com/2024/11/18/scubagear-open-source-tool-assess-microsoft-365-security/
DHS Releases Secure AI Framework for Critical Infrastructure	https://www.darkreading.com/cloud-security/dhs-releases-secure-ai-framework-critical-infrastructure

4 References

[1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), https://nvd.nist.gov/vuln-metrics/cvss

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.